Cybersecurity Policy Compliance: An Empirical Study of Jamaican Government Agencies

Donalds, Charlette, University of the West Indies, Mona, charlette.donalds02@uwimona.edu.jm

ABSTRACT

In addition to implementing technological tools, entities have adopted cybersecurity policies (CSPs) to address the rising number of employee related cybersecurity (CS) incidents. If however, employees do not understand the importance of or are unwilling to comply with CSPs, CS efforts may be in vain. This study investigates employees' actual CS compliance behaviour. Informed by the literatures on security behavioural interventions and organizational behaviour, this study is motivated by the fundamental premise that employee CS compliance is influenced by security behavioural intervention and organizational context factors. An integrated CS compliance model of CS awareness, CS training and top management support (TMS) is developed. The theoretical model is empirically validated with a data set representing the survey responses of employees in key Jamaican Government Agencies. The results from the structural equation modelling tests suggest that: (a) CS awareness is a significant factor contributing to employees' CS compliance behaviour; (b) the support and involvement of top management have a significant impact on CS compliance; and (c) CS training is a significant factor that influences CS awareness.

Keywords: Cybersecurity Compliance, Jamaica, Awareness, Top Management Support, Training

INTRODUCTION

Like in other jurisdictions, the Government of Jamaica (GOJ) recognizes the importance of information and communications technologies (ICTs) as powerful tools for sustainable socio-economic development. In its recently published National Development Plan (Vision 2030 Jamaica), the GOJ identifies a technology enabled society as one of its national outcomes

(Planning Institute of Jamaica, 2009). The GOJ's vision is that increased use and application of ICTs will drive productivity and efficiency. This is consistent with research that suggests a strong linkage between the levels of ICT advancement and growth in per capita GDP of the country (UNCTAD, 2006).

However, inherent with increased usage of ICTs, is increased potential of cybersecurity (CS) threats and attacks. Emerging trends in Jamaica demonstrate increasing cyber incidents. Reports from the Communication Forensics and Cybercrime Unit (CFCU) in the Jamaica Constabulary Force (JCF) show cyber incidents reported increasing some 78% in 2012 over 2011 (Government of Jamaica, 2015). Similarly, in 2012 there were 299 reported cases of website hacking while in comparison, none was reported in 2011 (Government of Jamaica, 2015). The increasing number of incidents indicates that CS is a real challenge for GOJ agencies and other Jamaican entities. The inability of the GOJ to deal with cyber attacks have the potential to erode confidence and trust in the use of ICTs and may hinder foreign direct investments, all of which may negatively influence the realization of national development.

The threat of CS attacks have prompted entities (private, public and government agencies) to actively use security technologies to protect information technology assets, however, CS cannot be achieved through technological tools alone. Entities have also established cybersecurity policies (CSPs) and procedures to mitigate intended or unintended behaviour of employees that could weaken or render technological based solutions useless. In general, CSPs define rules and guidelines for employees when utilizing the entities' information technologies to ensure protection of the entities' information technologies and information from cyber attacks. However, if employees do not comply with CSPs, the entities' information assets may not be secured. There is empirical evidence that information systems security policies (ISPs) positively influence users' computer abuse (Straub, 1990). While establishing CSPs may be a reasonable starting point, it is not sufficient to ensure employees' compliance with CSPs. Therefore, an understanding of what factors influence employees compliance with their entities' CSPs is essential for helping CS managers diagnose deficiencies in their CS management efforts and in providing them with information to improve compliance with CSPs.

While there has been some recent works investigating factors motivating employees' security policy compliance intention behaviour (Bulgurcu et al., 2010, Herath and Rao, 2009, Hu et al.,

2012), what has not been investigated, to the best of the researcher's knowledge, is employees actual compliance behaviour in the CS context. Except for Chan et al. (2005) who found that employee perceptions of the information security climate positively impact security policy compliance behaviour, little is known about employees' actual compliance behaviour.

The security literature emphasizes the need for managers to focus on awareness and training initiatives (Herath and Rao, 2009, Puhakainen and Siponen, 2010) in order to improve employees compliance behaviour. However, there is a paucity of empirical studies that investigates the impact of information security awareness (ISA) on compliance behaviour. The hypothesis that ISA influences employees compliance intention behaviour is empirically supported in prior research (Bulgurcu et al., 2010). However, it is not yet known whether awareness of CS threats and consequences directly influence employee compliance behaviour in the CS context. Further, awareness is cited as a key strategic objective of Jamaica's current National Cybersecurity Strategy (Government of Jamaica, 2015). In this strategy it is posited that CS awareness and CS training for employees' are critical factors for the successful realization of any security program generally and Jamaica's CS plan specifically. Thus, the results of this study would be of particular interest to CS managers in Jamaica's public sectors.

Training is another approach that has been used to address the concern of IS security compliance and is also conceptualized as influencing awareness. For instance, Siponen (2000) states that "awareness involves education and training"; education answers the "why" while training corresponds to the "how", and should increase skills and competence. Notwithstanding the fact that training is touted as one of the most commonly suggested approaches to address IS security compliance (Puhakainen and Siponen, 2010), the relationship between training and IS security compliance is not yet investigated. Like awareness, training too, to the best of the researcher's knowledge, has not yet been investigated in the CS context.

In the IS and security literatures, top management support (TMS) has emerged as a key construct. For instance, TMS is identified as: 1) a critical success factor for IS implementation success and use (Sabherwal et al., 2006); 2) influencing employee behaviour and outcome (Hu et al., 2012, Liang et al., 2007); 3) a significant predictor of organization's security culture and level of policy enforcement (Knapp et al., 2006); 4) positively related to IS security preventive efforts (Kankanhalli et al., 2003); and, 5) significantly affecting employees belief with respect to

ISPs and procedures (Hu et al., 2012). However, to the best of the researcher's knowledge, TMS has not yet been investigated in the CS context. Likewise, the influence of TMS on employee CS compliance behaviour is yet to be explored.

Given the critical role of TMS in the IS and security literatures and the influence of awareness and training on IS security behaviour, this study proposes an integrative model of CS compliance. This model is valuable for advancing our understanding of and for devising more effective strategies to improve CS compliance in organizations. In this model CS compliance is employees' perceptual measures of their actions toward protecting the information assets of the entity from potential CS attacks.

This study seeks to address the gaps in the literature by proposing a single integrative model to better understand employee CS compliance behaviour with consideration towards the organizational context and behavioural interventions aimed at mitigating CSPs breaches. Further, this study looks at actual compliance behaviour instead of compliance intention, which has been the focus of an emerging stream of research on individual security behaviour. Three research questions not yet investigated in the CS literature are addressed in this study: i) what influence does CS awareness have on employee actual compliance with CSPs? ii) what influence does TMS have on employee actual compliance with CSPs? iii) what influence does CS training have on CS awareness and employee actual compliance with CSPs? Data collected through a survey of 137 employees from 10 key GOJ agencies are used to answer the research questions.

The remainder of this study is organized as follows. The next section discusses the relevant literature followed by the conceptual foundation of the research. In the subsequent section, the research model is discussed and hypotheses to be tested are developed. The subsequent sections discuss the research design and methodology, a description of the data analysis and presentation of the results. Finally, the findings and implications for the research are discussed.

RELEVANT LITERATURE

A review of the security literature reveals that research on CS compliance has remained largely unexplored. Although it is recognized by academics and practitioners alike that employees are considered the weakest link in information security and by extension CS, they are also

considered to be great assets to reduce potential security risks and threats (Boss et al., 2009). However, little or no attention has been devoted to factors influencing CS compliance. That is, it is not well understood what factors influence adherence to the CSPs and procedures in organizations. Prior studies have instead focused on, albeit important security topics, as the design, development, and alignment of the ISP (Siponen and Iivari, 2006, Doherty and Fulford, 2006); the role of organizational commitment on various security-related behaviours (Stanton et al., 2003); the role of security climate on security policy compliance (Chan et al., 2005); IS security effectiveness (Kankanhalli et al., 2003); the influence of TMS on an organization's security culture and level of security policy enforcement (Knapp et al., 2006); and, end user security-related behaviours (Stanton et al., 2005).

To address the issue of non-compliance with ISPs, the use of sanctions, grounded in deterrence theory, has been widely investigated by IS scholars. For instance, Kankanhalli et al. (2003) found that greater deterrent efforts led to enhanced IS security effectiveness. Siponen et al. (2007) found that deterrents significantly influence employees' compliance with IS security policies. D'Arcy et al. (2009) found that computer monitoring, IS security policies and awareness programs influence perceived severity of formal sanctions, which led to reduced intention to misuse IS. While Herath et al. (2009) found that punishment severity had a significant impact on policy compliance intention, it had a negative effect. In contrast with empirical studies on compliance with IS security policies, Siponen et al. (2010) reported that formal sanctions did not influence IS security policy violations.

While the use of sanctions is a widely suggested approach to reduce computer abuse and improve employee compliance with IS security policies (Siponen and Vance, 2010), behavioural interventions are also suggested to address the IS security problem. One of the tasks of security managers is to promote positive changes in employees' security behaviour. Interventions to bring about these changes should be directed at employees' skills and knowledge pertinent to the security context. Two recommended behavioural interventions to address security breaches are, improving IS awareness and/or CS awareness (D'Arcy et al., 2009, Government of Jamaica, 2015, Hu et al., 2012, Mitnick, 2002, Siponen, 2000) and increasing training (Puhakainen and Siponen, 2010, Siponen, 2000, Thomson and von Solms, 1998). The aim therefore of CS awareness and training is to persuade employees and activate their thinking processes in such a

way that they internalize why it is important to comply with security policies and enable them to take necessary actions.

In this study CS awareness refers to the on-going efforts of the organization to develop employees understanding of the potential CS threats and risks they likely face and appropriate actions to take to protect the organization's information assets. Awareness mechanisms can include posters, newsletters, security briefings and notices. Although the importance and benefits of security awareness has long been espoused (Siponen, 2000, Straub and Welke, 1998), there is limited empirical evidence supporting these claims. D'Arcy et al. (2009) provide empirical evidence that user awareness of security policies; security education, training, and awareness (SETA) programs can help improve security adherence. Stanton (2005) reported that a greater degree of awareness was positively associated with changing passwords more frequently and choosing better passwords, providing some support for the beneficial effects of awareness on getting employees to improve security behaviour. Consistent with findings in other studies, Bulgurcu et al. (2010) provide empirical evidence that IS awareness exert significant influence on an employee's attitude toward compliance. Choi et al. (2013) suggested that cybersecurity counter measures awareness – users' awareness of computer monitoring, users' awareness of security training programs, users' awareness of security policies – influence computer misuse intention. They reported that users' awareness of computer monitoring influences computer misuse intention as well as CS computing skills and that users' awareness of security policies significantly contributes to cybersecurity action skills. Still, to the best of the researcher's knowledge, the direct role of CS awareness on employees' CS actual compliance behaviour has not yet been investigated.

Despite the importance of security training, there is a paucity of empirical studies that analyse the impact of security training on IS security generally. For instance, Puhakainen (2006) proposed a design theory for improving security training, Thomson et al. (1998) highlights the importance of security training and Cox et al. (2001) suggests training via Web-based tutorial for increasing security compliance in academic environments. In an empirical vein, Goodhue et al. (1991) provide empirical evidence that training improves employees' compliance with security policies. Similarly, Stanton (2005) found that training enforcement of an acceptable use policy had beneficial effects on getting end users to change their passwords more frequently and compose stronger passwords. D'Arcy et al. (2009) also found support that information security

training programs help reduce users' misuse intention. The influence of CS training on employees' CS actual compliance remains unexplored until now.

According to Boss et al. (2009) one of the noted causes of IS security failures is the lack of computer security training to develop users security awareness. Puhakainen et al. (2010) found that properly designed training programs improved employee awareness about the possible consequences of noncompliance towards established information security policies, resulting in an increased level of compliance. This suggests that security training influences security awareness. To the best of the researcher's knowledge, the influence of security training on security awareness has not yet been investigated.

TMS is identified as one of the most critical elements in IS security. For instance, by asserting that "the realization that information security is a corporate governance responsibility (the buck stops right at the top)" as Sin number 1 of 10 deadly sins of information security management, von Solms et al. (2004) support the view that TMS is indeed critical to IS security. Kankanhalli et al. (2003), Puhakainen et al. (2010) and Hu et al. (2012) are among the few studies that tested the effect of top management's role in the information security context. The results of a survey of IS managers by Kankanhalli et al. (2003) showed that organizations with stronger TMS were engaged in more preventative security efforts than organizations with weaker TMS. Puhakainen et al. (2010) found that one of the primary reasons why employees who ignored the policies that required encryption of emails was because of the perceived passiveness of the CEO in promoting and following the established information security policies. Using survey data Hu et al. (2012) found that top management participation in information security initiatives have a significant impact on employee security compliance intention behaviour.

Although some research has been done to test the effect of the afore-discussed factors in the IS security context, to the best of the researcher's knowledge, none of the said factors are investigated in the context of actual CS policy compliance. Too, a single integrated model is still lacking. This study undertakes an investigation of an integrated model in an attempt to advance our understanding of and to indicate the relevance of the factors proposed in the model for CS compliance.

CONCEPTUAL MODEL

The behaviour of interest in this study is employees' CS compliance with CSPs and procedures. However, the extant literature presented in the preceding section mostly focuses on individual compliance intention behaviour and factors that influence this behaviour. The use of deterrents (e.g. sanctions) is a widely suggested approach to influence security behaviour. The researcher argues however, that behavioural interventions can influence employees' CS compliance behaviour. While there is a paucity of empirical support that behavioural interventions influence individual compliance intention, the influence of these behavioural interventions has not been articulated and tested in the CS compliance context. Too, the extant literature on individual behaviour also reports that employee behaviour is also influenced by the organizational context. However, the linkages between behavioural interventions (i.e., awareness and training) and the organizational context (i.e., TMS) on employees' actual CS compliance behaviour have not been explored. Thus, the effects of CS awareness, CS training and TMS in the security context must be accounted for to fully understand employee actual CS behaviour and to develop effective CS management practices. To accomplish this, the researcher argues that it is necessary to integrate existing theories on awareness, training and TMS, which in turn influence employee CS compliance behaviour. The fundamental argument of this study is that CS awareness and CS training can influence employee CS compliance behaviour and that CS training too can influence CS awareness; the support provided by top management can affect employee's behaviour towards CS compliance. This logic is shown in Figure 1.

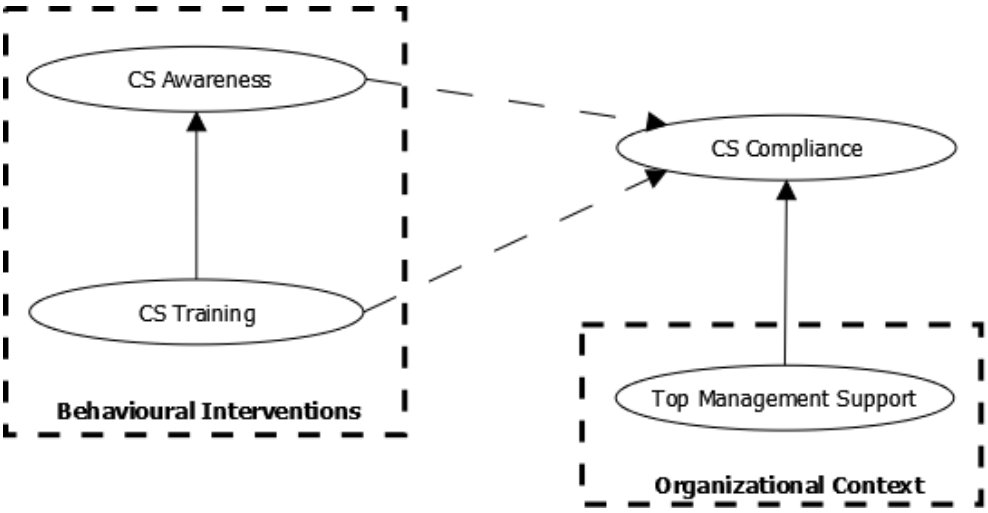

Figure 1. Conceptual model of CS compliance behaviour.

RESEARCH MODEL AND HYPOTHESES

Based on subsequent arguments below, the research model shown in Figure 2 is proposed.

Cybersecurity Awareness

According to Murray (1991) one of the biggest security problems is as a result of incompetence of employees who do not understand the dangers inherent in their actions. Researchers suggest increasing employees security awareness to overcome this problem (Hadland, 1998, Murray, 1991). According to Hansche (2001) the goal of a security awareness program is to heighten the importance of information systems security and the possible negative effects of a security breach or failure. For instance, employees can be made aware of the critical nature of data security and their responsibility to respect and protect the privacy of information, its integrity and confidentiality. Similarly, employees can be made aware of CS incident reporting procedure in the event a computer becomes infected by a virus or if they receive an illegitimate warning message or alert. Therefore, the argument made by Hansche (2001) that employees who are aware of IS security issues are the single most important asset for detecting and preventing IS security incidents, is a reasonable one. Likewise, in this study the researcher argues that employees' CS awareness is crucial for detecting and preventing potential CS threats and for reporting actual CS incidents.

The argument has been made that security awareness has the potential to influence behavioural outcomes. For instance, Siponen (2000) suggests that providing security awareness is the most important factor in persuading employees to change their compliance actions. Empirical evidence supports this claim as Stanton (2005) reports statistically significant correlations between password-related behaviours and awareness. The researcher therefore argues that providing CS awareness should influence employees to comply with CSPs and procedures. Hence, the hypothesis:

H1: CS awareness will positively influence actual CS compliance.

Cybersecurity Training

The security literature places strong emphasis on training for enabling security compliance behaviour (Siponen, 2000, Thomson and von Solms, 1998, Puhakainen and Siponen, 2010). For instance, Mitnick et al. (2002) argue for an on-going IS security training program as a means to resist social engineering. Further, Mitnick et al. (2002) argue that the goal of the training program is to influence employees to change their behaviours by motivating them to protect the IS asset of the company. This argument is consistent with findings of other researchers who found security training to significantly improve ISP compliance level (Puhakainen and Siponen, 2010). New hires should be provided CS training and at regular intervals thereafter to improve their abilities to perform the necessary CS related actions. For instance, employees may require training to select a strong password, i.e., passwords should be cryptic so they cannot be easily guessed but should be easily remembered and need not be written down. These abilities have been found to significantly affect compliance intention (Herath and Rao, 2009, Bulgurcu et al., 2010). Therefore, it is likely that training results in improved abilities while the absence of training can represent a barrier to undertaking an action, resulting in reduced adherence of CS compliance. Hence, the hypothesis:

H2: CS training will positively influence actual CS compliance.

It is also suggested that training is likely to remind employees of the organizational views of information security and emphasize its importance (Herath and Rao, 2009); thereby, heightening awareness of CSPs and procedures. Hadland (1998) suggests that training programs can be used to improve employees' awareness of existing IS security practices. These assertions imply that training influences awareness. In this study the researcher therefore argues that CS training will have a positive influence on CS awareness, hence the hypothesis:

H3: CS training will positively influence actual CS awareness.

Top Management Support

The role of top management in the CS context is to set organizational CS goals, such as the CSPs and procedures, provide resources for their successful establishment and resolves CS issues among different stakeholders. TMS is demonstrated via top management's actions such as the championing of initiatives, providing financial and political resources, making decisions

congruent with security policies and procedures, hold lower level managers accountable for non-compliance and communicate the seriousness and risks of non-compliance and securing legitimacy (Gomes et al., 2001, Hu et al., 2012). TMS demonstrates the commitment of the organization towards an initiative. For instance, Hu et al. (2012) argue that top management's involvement in security initiatives can send a strong signal to other managers and employees about the legitimacy of the initiatives. In fact top management involvement in security initiatives have been found to influence security compliance intention (Hu et al., 2012, Siponen and Vance, 2010) and security policy enforcement (Knapp et al., 2006).

Top management's active involvement in security initiatives and programs could be effective in motivating employees to commit to compliance behaviour. Puhakainen et al. (2010) provide evidence that TMS of established ISP affects employees behaviour and results in higher levels of compliance. Therefore, the researcher argues that top management support and active involvement in CS policies and procedures will positively influence employees actual CS compliance behaviour. Thus:

H4: Top management support will positively influence actual CS compliance.

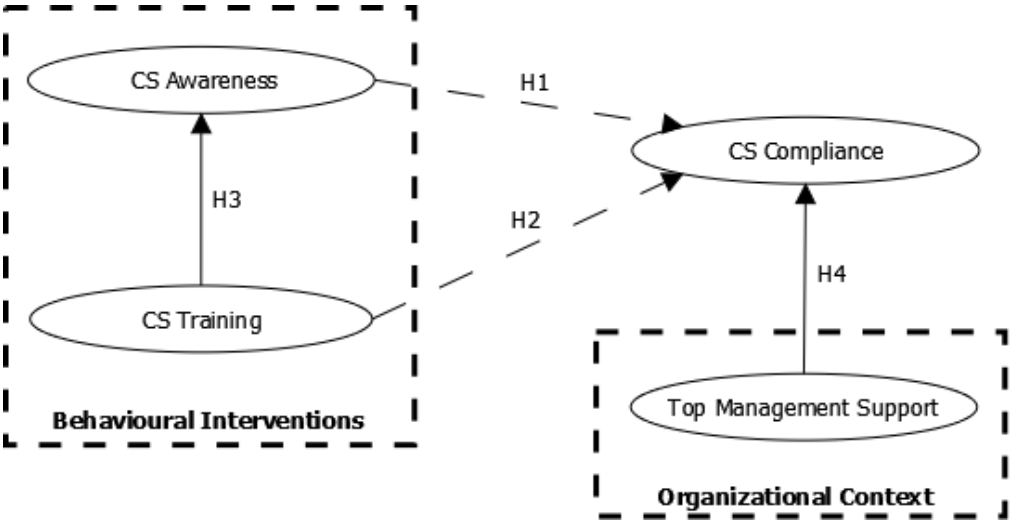

Figure 2. Research model.

RESEARCH METHOD AND DATA

Construct Operationalization

The survey instrument was developed based on the research model shown in Figure 2. Measurement items for each construct are based on a 7-point Likert like scale and are adapted from the extant literature to maximize validity and reliability of the measurement tool. All constructs in the model are operationalized as reflective constructs.

Data Collection

Data from a pilot study using employees in three GOJ agencies were used to refine the survey instrument. Minor changes were made to items that showed low loading in the initial analyses. The final version of the survey was administered in 10 GOJ agencies. The researcher requested a manager from each agency to randomly distribute 40 questionnaires to employees at varying levels in the agencies. Of the 400 questionnaires distributed, 166 were returned but only 137 were usable, yielding a response rate of 37%. Descriptive statistics showing the demographic profiles of the respondents are shown in Table 1.

Category	Subcategory	Count	Percentage (%)	Category	Subcategory	Count	Percentage (%)
Gender:				Job Level:			
	Male	68	50		Line Staff	81	59
	Female	69	50		Supervisor	25	18
Age:					Manager	26	19
	<30	49	36		GM/HOD	5	4
	30-49	78	57	Job Type:			
	>=50	10	7		Operational	57	42
Education:					Administrative	25	18
	High School	14	10		IT	55	40
	Diploma	22	16	Organization Tenure:			
	Undergraduate	76	55		<5 years	49	36
	Graduate	25	18		5-15 years	68	50
					>15 years	20	15

Table 1. Respondent demographics.

DATA ANALYSES AND RESULTS

Partial least square (PLS) is the analytic technique used. The PLS approach is appropriate for this study as it is well suited for assessing complex predictive models (Henseler et al., 2009). SmartPLS 2.0 M3 (Ringle et al., 2005) is the statistical tool used to analyse the measurement model as well as the path model for hypothesis testing.

Measurement Model

Reliability and validity tests are conducted to assess the outer model. All loadings are well above the threshold value of 0.7 and are significant at the 0.01 level, based on their t-values. Indicator reliability ranged from 0.733 to 0.972. The composite reliability values ranged from 0.914 to 0.971, demonstrating that the constructs have high levels of internal consistency reliability. Table 2 shows some quality indicators of the outer model.

Convergent validity is assessed using the AVE values (Chin, 1998, Fornell and Larcker, 1981). The AVE for each latent construct is well above 0.5 (see Table 2), indicating that the latent construct can account for at least 50% of the variance in the items.

Latent Construct	Item	Loading	*t* Value	AVE	Composite Reliability	Cronbach's Alpha
CS Awareness	CA1	0.889	25.0367	0.779	0.914	0.858
	CA2	0.863	24.2431			
	CA3	0.897	29.9477			
CS Training	TNG1	0.940	28.3957	0.893	0.971	0.960
	TNG2	0.938	31.1365			
	TNG3	0.972	87.2407			
	TNG4	0.931	27.3546			
Top Management Support	TMS1	0.841	14.9494	0.759	0.956	0.947
	TMS2	0.936	43.5658			
	TMS3	0.901	34.738			
	TMS4	0.875	26.9259			
	TMS5	0.922	47.3845			
	TMS6	0.785	6.2835			
	TMS7	0.829	14.1707			
CS Compliance	CC1	0.951	81.9976	0.783	0.915	0.859
	CC2	0.952	52.2668			
	CC3	0.733	4.1382			

Table 2. Measurement model indicators.

Discriminant validity can be assessed using the Fornell-Larcker criterion (i.e., the square root of the AVE) and cross loadings (Hair et al., 2014). Discriminant validity is achieved as the square root of the AVE for each construct is larger on itself than any number in the same row and column (see Table 3). The loadings of items on each construct is higher than all of its cross loadings with other constructs, also establishing discriminant validity.

	CS Awareness	CS Compliance	Top Management Support	CS Training
CS Awareness	**0.883**			
CS Compliance	0.544	**0.885**		
Top Management Support	0.453	0.587	**0.871**	
CS Training	0.371	0.450	0.575	**0.945**

Table 3. Latent variable correlations. Note: Values on the diagonal and bold are AVEs.

Structural Model

Figure 3 presents the estimates obtained from the PLS analysis. The R^2 value of 0.45 indicates that the model explains a substantial amount of variance in CS compliance. Figure 3 also shows that CS awareness – CS compliance and TMS – CS compliance are significant, supporting H1 and H4. The results also provide evidence for H3 since CS Training – CS awareness is significant. Although CS training influences CS awareness, it explains only 0.14 of the variance in CS awareness. Further, Figure 3 shows that CS training – CS compliance is insignificant, providing no support for H2.

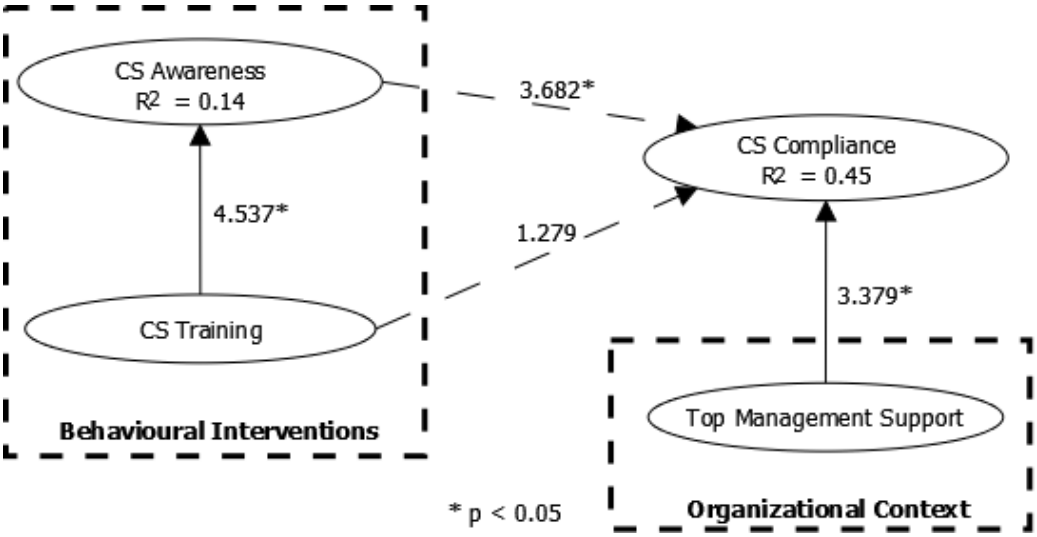

Figure 2. PLS analysis of results.

DISCUSSION

Although the overall thesis of the study is supported by the empirical evidence, the insignificance of the relationship between CS training and CS compliance deserves further discussion. According to Puhakainen et al. (2010) training programs that are designed based on information security theoretical underpinnings are usually more effective than generic training programs of information security technologies and policies. Perhaps the training provided by GOJ agencies were too generic and so did not achieve the desired effect, i.e., directly influencing employees' actual CS behaviour. Puhakainen et al. (2010) also suggest that for training to be effective, it should be continuous and integrated into the organization's normal communication effort, however, in this study these suggestions were not investigated.

THEORETICAL CONTRIBUTIONS

While employees' information security compliance intention is given some focus in the literature (Bulgurcu et al., 2010, D'Arcy et al., 2009, Herath and Rao, 2009, Puhakainen and Siponen, 2010, Hu et al., 2012), what is less understood is employee's actual compliance behaviour. Four key aspects of this study signify our contribution to the theory of actual compliance behaviour. First is the focus on actual compliance behaviour in the context of CS. Second, this study

integrates CS awareness, TMS and CS training into one model. In existing information security literature, TMS, awareness and training were not previously studied together. Third, a new relationship for adding to the nomological net of CS, and by extension, to information security models: CS training – CS awareness. Fourth, to the best of the researcher's knowledge, this is the first study that has empirically shown the effect of TMS, awareness and training on employees' actual compliance behaviour in the CS context.

MANAGERIAL IMPLICATIONS

The findings offer guidance to management and IT practitioners in GOJ entities and organizations in other jurisdictions. The direct influence of TMS on compliance clearly highlights the critical role of top management in CS. This finding demonstrates that active and visible involvement of top management can have a positive influence on employees' actual compliance. Second, the significant influence of awareness suggests that implementing awareness programs in organizations will have a positive impact on employees' actual CS compliance behaviour. Finally, the results also suggest to managers that although it is certainly important to have CS training programs, they are not sufficient to directly influence employees' actual compliance behaviour with the CSPs. In fact, the results suggest that CS awareness mediates the relationship between CS training and CS compliance.

LIMITATIONS AND FUTURE RESEARCH

There are limitations to the study. For instance, it has been suggested that information security assurance will require a multifaceted approach encompassing both social and technical factors (Dhillon and Backhouse, 2001). Likewise, the GOJ National Cybersecurity Plan also suggests a multifaceted approach. However, this study does not consider such factor as organization climate, which has been shown to influence other organization phenomenon such as individual performance (Donalds, 2010). Incorporating social factors in future studies may improve our understanding of what influences employee actual CS compliance. The model proposed in this study was tested using employees' perceptual measures of CS compliance. However, there can

be discrepancy between self-reports and actual behaviours and therefore it is not known how well the respondents' perceptions matched their actual compliance behaviours. In a follow-up study objective measures could be used, however, this may increase the risk of response bias.

CONCLUSION

In this study an employee actual CS compliance model is developed by integrating factors relevant to employee actual behaviour: TMS, CS awareness and CS training. The effect of CS training on CS awareness and CS training and CS compliance are also considered. Using survey data and structural equation modelling, hypothesis test on whether TMS influences CS compliance was conducted and was confirmed. Also confirmed is that CS awareness significantly influences actual CS compliance behaviour with CSPs. Further, the influence of CS training on CS awareness was also supported.

This study is one of the first, if not the first empirical study to investigate actual compliance behaviour in the CS context. Additionally, it advances a long stream of research on individual information security compliance by examining actual behaviour instead of behavioural intention. Further, this study adapted factors from the information security and organizational literatures and integrate these into a single comprehensive model which was empirically validated. The study also offers one relationship for addition to the nomological net of information security and future CS compliance behaviour models.

REFERENCES

Boss, S. R., L. J. Kirsch, I. Angermeier, R. A. Shingler and R. W. Boss (2009). "If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security." *European Journal of Information Systems* 18**,** 151–164.

Bulgurcu, B., H. Cavusoglu and I. Benbasat (2010). "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness." *MIS Quarterly* 34 (3)**,** 523-548.

Chan, M., I. Woon and A. Kankanhalli (2005). "Perceptions of information security in the workplace: Linking information security climate to compliant behavior." *Journal of Information Privacy & Security* 1 (3)**,** 18-41.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *In:* MARCOULIDES, G. A. (ed.) *Modern methods for business research.* Mahwah, NJ: Lawrence Erlbaum Associates.

Choi, M. S., Y. Levy and A. Hovav (2013). "The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse." *Eighth Pre-ICIS Workshop on Information Security and Privacy (WISP2013).* Milan, Italy.

Cox, A., S. Connolly and J. Currall (2001). "Raising IS security awareness in the academic setting." *VINE* 31 (2)**,** 11-16.

D'Arcy, J., A. Hovav and D. Galletta (2009). "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach." *Information Systems Research* 20 (1)**,** 79-98.

Dhillon, G. and J. Backhouse (2001). "Current direction in IS security research: Towards socio-organizational perspective." *Information Systems Journal* 11 (2)**,** 127-153.

Doherty, N. F. and H. Fulford (2006). "Aligning the information security policy with the strategic information systems plan." *Computers and Security* 25 (1)**,** 55-63.

Donalds, C. (2010). "46p. Towards an ERP individual performance model." *CONF-IRM 2010 Proceedings.* Montego Bay, Jamaica.

Fornell, C. and D. F. Larcker (1981). "Evaluating structural equation models with unobservable variables and measurement error." *Journal of Marketing Research* 18 (1)**,** 39-50.

Gomes, J., P. De Weerd-Nederhof, A. Pearson and O. Fisscher (2001). "Senior management support in the new product development process." *Creativity and Innovation Management* 10 (4)**,** 234-242.

Goodhue, D. L. and D. W. Straub (1991). "Security concerns of system users: A study of perceptions of the adequacy of security." *Information & Management* 20 (1)**,** 13- 27.

Government of Jamaica. (2015). Jamaica national cyber security strategy. Available: http://www.mstem.gov.jm/sites/default/files/documents/Jamaica%20National%20Cyber%20Security%20Strategy.pdf [Accessed Janauary 28, 2015].

Hadland, T. (1998). "IS security management: An awareness campaign." *In:* ARMSTRONG, C. J. & HARTLEY, R. J. (eds.) *UKOLUG98: New Networks, Old Information—UKOLUG's 20th Birthday Conference.* Manchester, England.

Hair, J. F., G. T. M. Hult, C. M. Ringle and M. Sarstedt (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*, Thousand Oaks: Sage.

Hansche, S. (2001). "Designing a security awareness program: Part 1." *Information Systems Security* 9 (6)**,** 14-22.

Henseler, J., C. M. Ringle and R. R. Sinkovics (2009). The use of partial least squares path modeling in international marketing. *In:* SINKOVICS, R. R. & GHAURI, P. N. (eds.) *Advances in international marketing.* Emerald Group Publishing Limited.

Herath, T. and H. R. Rao (2009). "Protection motivation and deterrence: A framework for security policy compliance in organisations." *European Journal of Information Systems* 18**,** 106–125.

Hu, Q., T. Dinev, P. Hart and D. Cooke (2012). "Managing employee compliance with information security policies: The critical role of top management and organizational culture." *Decision Sciences* 43 (4)**,** 615-659.

Kankanhalli, A., H.-H. Teo, B. C. Y. Tan and K.-K. Wei (2003). "An integrative study of information systems security effectiveness." *International Journal of Information Management* 23 (2)**,** 139-154.

Knapp, K., T. E. Marshall, R. K. Rainer and F. N. Ford (2006). "Information security: Management's effect on culture and policy." *Information Management & Computer Security* 14 (1)**,** 24-36.

Liang, H., N. Saraf, Q. Hu and Y. Xue (2007). "Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management." *MIS Quarterly* 31 (1)**,** 59-87.

Mitnick, K. D. and W. L. Simon (2002). *The art of deception: Controlling the human element of security*, USA, Wiley Publishing.

Murray, B. (1991). "Running corporate and national security awareness programs." *IFIP TC11 Seventh International Conference on IS Security.* Amsterdam: North-Holland Publishing Co.

Planning Institute of Jamaica (2009). "Vision 2030 Jamaica: National development plan." Jamaica: Planning Institute of Jamaica.

Puhakainen, P. (2006). *A design theory for information security awareness.* PhD, University of Oulu, Finland.

Puhakainen, P. and M. Siponen (2010). "Improving employees' compliance through information systems security training: An action research study." *MIS Quarterly* 34 (4)**,** 757-778.

Ringle, C. M., S. Wende and A. Will (2005). "SmartPLS 2.0 M3." Hamburg, Germany: SmartPLS.

Sabherwal, R., A. Jeyaraj and C. Chowa (2006). "Information system success: Individual and organizational determinants." *Management Science* 52 (12)**,** 1849-1864.

Siponen, M. (2000). "A conceptual foundation for organizational information security awareness." *Information Management & Computer Security Journal* 8 (1)**,** 31-41.

Siponen, M. and J. Iivari (2006). "Six design theories for IS security policies and guidelines." *Journal of the Association for Information Systems* 7 (7)**,** 445-472.

Siponen, M., S. Pahnila and A. Mahmood (2007). "Employees' adherence to information security policies: An empirical study." *IFIP SEC 2007.* Sandton, Gauteng, South Africa.

Siponen, M. and A. Vance (2010). "Neutralization: New insights into the problem of employee information systems security policy violations." *MIS Quarterly* 34 (3)**,** 487-502.

Stanton, J. M., K. Stam, I. Guzman and C. Caldera (2003). "Examining the linkages between organizational commitment and information security." *IEEE Systems, Man, and Cybernetics Conference.* Washington, DC, USA.

Stanton, J. M., K. R. Stam, P. Mastrangelo and J. Jolton (2005). "Analysis of end user security behaviors." *Computers & Security* 24 (2)**,** 124-133.

Straub, D. (1990). "Effective IS security: An empirical study." *Information Systems Research* 1 (3)**,** 255-276.

Straub, D. W. and R. J. Welke (1998). "Coping with systems risk: Security planning models for management decision making." *MIS Quarterly* 22 (4)**,** 441-469.

Thomson, M. E. and R. Von Solms (1998). "IS security awareness: Educating your users effectively." *Information Management & Computer Security* 6 (4)**,** 167-173.

Unctad. (2006). Wir06. FDI from developing and transition economies: Implications for development. Available: http://unctad.org/en/docs/wir2006_en.pdf [Accessed December 6, 2014].

von Solms, B. and R. von Solms (2004). "The 10 deadly sins of information security management." *Computers & Security* 23 (5)**,** 371-376.